Department of Homeland Security Daily Open Source Infrastructure Report for 08 March 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- Federal and state authorities expect to close a 50−person Colorado counterfeit documents ring allegedly masterminded by a Mexico−based crime family, crafting millions of dollars worth of fake IDs, including fake documents used by illegal aliens to purchase 300 homes valued at $51 million. (See item 12)
- The Pew Hispanic Center, in a new report, states the number of illegal immigrants in the United States has grown to as many as 12 million, and now account for about one in every 20 workers. (See item 14)
- The Associated Press reports two commercial airliners came too close to each other on Sunday, March 5, as they prepared to land on separate runways at Nashville International Airport. (See item 15)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *March 07, Energy Information Administration* — **EIA releases March 2006 Short−term Energy Outlook.** The Energy Information Administration estimates that world spare oil production capacity is projected to increase only modestly during 2006 and 2007 despite new

supplies from both non−OPEC and OPEC countries. Outside of the United States, net production increases in 2006 of 100,000 to 200,000 barrels per day (bbl/d) are expected in the Caspian, Canada, Angola, Russia, Brazil, and Mexico areas. According to the Minerals Management Service, approximately 400 million cubic feet per day of natural gas production are expected to remain offline prior to the start of the next hurricane season, June 1, 2006. However, overall dry gas production is projected to increase by 2.2 percent in 2006 and 1.7 percent in 2007. Total liquefied natural gas (LNG) imports are projected to increase from their 2005 level of 630 billion cubic feet (BCF) to 830 bcf in 2006. LNG imports in 2007 are expected to reach 1,030 bcf.
Source: http://www.eia.doe.gov/steo

2. *March 05, Reuters* — **Camisea gas pipe leaks for fifth time in Peru.** Peru's Camisea gas pipeline has leaked for the fifth time in 18 months, causing a fire and injuring two people, its operator said on Sunday, March 5, following warnings of ruptures because of poor pipe construction. Pipeline operator Transportadora de Gas del Peru (TgP) said the 430−mile pipe on Saturday, March 4 leaked 750 cubic meters of natural gas in Peru's southern jungle region. "The estimated volume of liquid lost is 750 cubic meters. A fire also broke out at the leakage point, which is burning up the spilled liquid," TgP said in a statement. Peru's Prime Minister Pedro Pablo Kuczynski said the leak may have been caused by sabotage on the pipeline. The pipeline, which was built with Inter−American Development Bank funding, has leaked five times since it began pumping natural gas in mid−2004. E−Tech International last week warned the pipeline was likely to leak at six points because of rusty, badly welded pipes. Hunt Oil of the United States is among several partners in TgP. The pipeline previously leaked in November, spilling 6,000 barrels of fuel into the jungle, according to the government, which has warned TgP it could cancel its operating contract if future leaks occur.
Source: http://news.yahoo.com/s/nm/20060305/sc_nm/energy_peru_camise a_dc_1

3. *March 03, KUAM 8 News (Guam)* — **Theft of copper wire getting dangerous.** Guam has been plagued by a rash of recent thefts of copper wire, and according to the Guam Power Authority (GPA) several thousand feet of copper wire has been cut off of live lines. Adding to this is the recent theft of some aluminum materials from a GPA substation. A few weeks ago the utility agency was burglarized when thieves began stealing copper wire. Consolidated Commission on Utilities spokesperson Art Perez says that approximately 8,000 feet of wire has been stolen from the areas of Latte Estates, the Harmon Cliffline, and along Ysengsong Road in Dededo. Perez adds that this copper wire is being lifted directly off of live power poles, something extremely dangerous. Said Perez, "The thieves cut the wire mid−span...that means within the length of two poles cut mid−span left dangling and left hot with no regard to who might come in contact with these lines." Now Perez says that burglars have recently hit a Guam Waterworks Authority substation in Windward Hills, explaining, "Aluminum shutters that are used to protect emergency generators that power up these water pumps during typhoon restorations and disaster recoveries were stolen."
Source: http://www.kuam.com/news/16976.aspx

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *March 06, Mercury News (CA)* — **Pool chemical leak sends seven to hospital.** About 50 students and teachers at two Sunnyvale, CA, schools complained of discomfort and seven of them were taken to hospitals Monday afternoon, March 6, after a chemical leak at the King's Academy swimming pool. Chlorine and hydrochloric acid used to clean the pool leaked from their holding tanks and mixed together, Sunnyvale Lt. Marty Dale said. Children were evacuated from the Rainbow Montessori School, and taken to the theater at King's Academy. Residents within a six−block area around the schools were notified of the leak by phone and advised to stay indoors.
   Source: http://www.mercurynews.com/mld/mercurynews/news/local/140349 62.htm

[Return to top]

Defense Industrial Base Sector

5. *March 07, Reuters* — **EU takes first step on research fund.** European Union (EU) defense ministers gave their backing to a proposed common fund for defense research on Tuesday, March 7, in a rare move towards pooling the bloc's jealously guarded national military budgets. Britain, a top spender in the area, said it would initially not divert money to the project, aimed at narrowing the United States' burgeoning technology lead, but gave its blessing as a way to encourage other European states to spend more. European leaders will decide whether to give the fund final approval at a summit scheduled for June. While the money involved will be minimal compared to U.S. defense research spending, analysts say any decision to start such a fund could be a landmark precursor to much greater coordination of EU defense spending in the long run.
   Source: http://www.defensenews.com/story.php?F=1581196&C=europe

6. *March 06, Congress Daily* — **Army seeks to restore $3 billion for tank upgrades.** The Army has given Congress a $7.4 billion wish list of programs that did not make the Bush administration's request for either the fiscal 2006 wartime supplemental appropriations or fiscal 2007 defense budget request. The Army's so−called unfunded requirements list, delivered Friday, March 3, and larger than ones from the other armed services, includes $3 billion in heavy armor upgrades that had been dropped at the last minute from the requested supplemental. Army leaders say they need another $331.9 million to buy 96 M88 Improved Recovery Vehicles, enough to outfit four combat brigades. The Army also wants $331.5 million to buy 12 Boeing CH−47 Chinook helicopters and $71 million for five UH−60 Blackhawk helicopters to replace choppers lost in combat.
   Source: http://www.govexec.com/story_page.cfm?articleid=33549&dcn=to daysnews

[Return to top]

Banking and Finance Sector

7. *March 07, Finextra* — **Citibank blocks ATM cards after retailer breach.** Citibank has imposed transaction blocks on an unspecified number of U.S. card accounts after suffering a series of fraudulent cash withdrawals at ATMS in the UK, Russia, and Canada. News of the security scare spread rapidly after a Citibank customer reported the problems in a blog update.

Citi has indicated that the security problems stem from a previous breach at a U.S. retailer. The bank says in a statement, "Recently, we became aware of fraudulent ATM cash withdrawals on Citi−branded MasterCard credit and debit cards used in three countries on customer accounts that had been possibly compromised in previous retailer breaches in the U.S... To protect customer accounts that were affected, we placed a special transaction block in those three countries on PIN based transactions. We are currently reissuing cards, as appropriate, to affected customers." The bank not identified the afflicted retailer or quantify the number of customer card accounts affected.
Source: http://www.finextra.com/fullstory.asp?id=15014

8. *March 07, Finextra* — **UK phishing fraud losses double.** Direct fraud losses from online phishing scams in the UK almost doubled in 2005, according to statistics from the Association for Payment Clearing Services (APACS). The APACS says the introduction of chip and PIN technology has helped cut credit and debit card fraud for the first time in a decade, but organized gangs of scammers are now increasingly targeting the Web. Losses from Web banking fraud −− which are mainly the result of phishing scams −− rose 90 percent in 2005. Rising phishing fraud losses have prompted some banks in the UK to roll out extra security to customers. Last week Alliance and Leicester said it is introducing a form of two−factor authentication across all of its Internet accounts. Lloyds TSB has conducted trials of a Vasco two−factor authentication device which it says was a success. In addition to reducing losses from phishing scams, the system is expected to cut card−not−present (CNP) fraud, which jumped 21 percent in 2005. APACS claims the rate of increase for CNP fraud has fallen for the first time since 2003, due in part to e−retailers checking cardholder addresses.
Source: http://www.finextra.com/fullstory.asp?id=15013

9. *March 06, Associated Press* — **Three Colombians indicted on drug, money laundering charges.** Three Colombians have been charged with drug trafficking and money laundering in a U.S. grand jury indictment and have already been arrested in their home country, federal officials said. The three were charged in a 49−count indictment with laundering more than $3 million in drug proceeds through U.S. banks beginning in 2002 for cocaine distribution rings in Colombia, Mexico, and Europe. The suspects were identified as Ricardo Mauricio Bernal Palacios, Juan Manual Bernal Palacios, and Camilo Andres Ortiz Echeverri. They allegedly operated from Bogota, Colombia, and Mexico City. All three were arrested last Thursday, March 2, in Bogota and must be extradited to face the U.S. charges in Miami.
Source: http://www.sun−sentinel.com/news/local/miami/sfl−0306indicte dcolombians,0,3080609.story?coll=sfla−news−miami

10. *March 06, Buffalo News (NY)* — **Fuel retailers fighting card fraud with zip codes.** With credit card fraud in the U.S. costing an estimated $1 billion per year, gas stations are beginning to use zip codes to automatically authorize credit card payments. If the zip code the cardholder provides when making a fuel purchase fails to match that for the card's billing address, the transaction is denied. As card payments at self−service devices such as pay−at−pump fuel purchases or ticket machines often do not require a signature, zip codes are increasing as a cardholder verification method, much like PIN−secured card payments are in the UK. In the mainstream retail market, big names such as Best Buy, Kmart and JC Penney have for some time requested zip codes or photo ID at the POS for large card purchases. This practice appears to be shifting to self−service card payments, but is ineffective against fraud in cases where a

card thief obtains both a card number and the cardholder's address.
Source: http://www.epaynews.com/index.cgi?survey=&ref=browse&f=view&id=11416539196222152 12&block=

11. *March 06, Washington Post* — **Street−level credit card fraud.** Thieves in Las Vegas, NV, are encoding hotel room keys with stolen financial data, including 16−digit credit card numbers, date, person's name, and the name of a bank. The keys function exactly like credit cards, allowing the carrier to pay for merchandise at any store or market where customers do their own swiping. The idea is to be able to anonymously use someone else's credit card at a physical location; hotel room keys are likely to be overlooked or set aside for what they appear to be. "It was getting fairly regular that in post−arrest inventory, we would find eight to 10 room key cards ... all from different hotels," said Dennis Cobb of the Las Vegas Metropolitan Police Department. "The people who had these cards on them were using them in transactions with local businesses," Cobb said. The discovery led Cobb's division to team up with researchers from the Identity Theft and Financial Fraud Research and Operations Center at the University of Nevada, Las Vegas to devise technologies that police could deploy in the field to detect various types of fraud.
Source: http://blog.washingtonpost.com/securityfix/2006/03/street_level_credit_card_fraud.html

12. *March 03, Denver Business Journal (CO)* — **Crime franchise hub in Colorado.** Federal and state authorities hope to close a 50−person Denver counterfeit documents ring allegedly masterminded by a Mexico−based crime family they believe operates in at least 33 states, crafting millions of dollars worth of fake IDs, including fake documents used by illegal aliens to purchase 300 homes valued at $51 million. Authorities say that document forgers paid "franchise fees" of $15,000 a month to participate in the phony documents network. Investigators from the Department of Homeland Security, the U.S. Immigration and Customs Enforcement and other agencies have been shutting down "cell" operations. "This criminal organization represents one of the largest and most sophisticated document fraud rings ever uncovered −− so much so that it set up franchises in most major U.S. cities and counterfeited dozens of types of documents," said Marcy Forman of the U.S. Immigration and Customs Enforcement. The workers allegedly created one−stop shopping for everything from fake alien registration cards to Social Security cards, counterfeit drivers' licenses, birth certificates and insurance cards, said Carl Rusnock, a spokesperson for U.S. Immigration and Customs Enforcement. American Express Corp. lost approximately $2 million from the fraudulent operations. Such documents spark concerns that banks could unknowingly lend money to unqualified borrowers.
Source: http://www.bizjournals.com/denver/stories/2006/03/06/story3. html?t=printable

[Return to top]

Transportation and Border Security Sector

13. *March 07, Associated Press* — **Homeland Security gives port town surveillance power.** Dillingham, a fishing village in Southwest Alaska, now has 80 surveillance cameras, focused mainly on the port, courtesy of a $202,000 Department of Homeland Security federal grant. Dillingham Police Chief Richard Thompson said the cameras could stop terrorism in Southwest

Alaska someday. In addition, they may also put an end to the drinking, deaths, and drug deals that go on at the port every summer when the town fills up with commercial fishermen. The cameras are mostly aimed at the port, the chief said. About three−dozen cameras watch from poles there. Another seven watch the harbor from City Hall.
Source: http://159.54.227.3/apps/pbcs.dll/article?AID=/20060307/NEWS 06/60307030

14. *March 07, Associated Press* — **Number of illegal immigrants hits 12M.** The number of illegal immigrants in the United States has grown to as many as 12 million, and they now account for about one in every 20 workers, a new estimate says. Efforts to curb illegal immigration have not slowed the pace, said a report Tuesday, March 7, by the Pew Hispanic Center. Instead, the report's author said, those efforts are having an unintended consequence: People who illegally enter the United States from Mexico are staying longer because it is harder to move back and forth across the border. "The security has done more to keep people from going back to Mexico than it has to keep them from coming in," said Jeffrey Passel, a senior research associate at the center. The report estimates that 850,000 illegal immigrants have arrived in United States each year since 2000. There are about 7.2 million undocumented workers in the U.S., or about five percent of the country's work force, the Pew report said. Tuesday's report said Mexicans make up 56 percent of illegal immigrants. An additional 22 percent come from other Latin American countries, mainly in Central America. About 13 percent are from Asia, and Europe, and Canada combine for six percent.
Pew Hispanic Center Report: http://pewhispanic.org/reports/report.php?ReportID=61
Source: http://www.sacbee.com/24hour/politics/story/3220932p−1194397 5c.html

15. *March 07, Associated Press* — **Airlines report close call between planes landing at Nashville.** Two commercial airliners came close to each other Sunday, March 5, as they prepared to land on separate runways at Nashville International Airport. The Northwest Airlines and Southwest Airlines planes were eight miles from the airport when they got close enough to sound an alarm in the Northwest cockpit, WSMV−TV of Nashville reported. The Southwest 737 was en route from Austin, TX, and was carrying 137 passengers and a crew of five. The Northwest plane was en route from Detroit with 86 passengers and a crew of four. As the Northwest flight approached its runway, the Southwest flight threatened to cross its path, the station reported. The Northwest pilots made a descent before landing to avoid the Southwest plane. The Federal Aviation Administration is investigating.
Source: http://www.usatoday.com/travel/flights/2006−03−07−nashville− close−call_x.htm

16. *March 07, Reuters* — **Delta adds JFK flights as part of overseas push.** Delta Air Lines Inc. said on Tuesday, March 7, it would increase flights to New York's JFK International Airport in a bid to bring more passengers to higher−margin routes to Europe and other destinations. Delta, which is trying to recover profitability after soaring fuel prices and stiff domestic competition drove it into bankruptcy, said 46 additional daily flights from 17 cities would begin between June and September. Separately, recently filed court documents show that lawyers, advisers and accountants in the carrier's bankruptcy case have run up bills of about $41.8 million from September 2005 through January. The airline, based in Atlanta, filed for bankruptcy protection in September, and has been focusing on its international routes, where discount carriers do not fly.
Source: http://today.reuters.com/investing/financeArticle.aspx?type= bondsNews&storyID=2006−03−07T201653Z_01_N07168275_RTRIDST_0_

AIRLINES-DELTA-UPDATE-2.XML

17. *March 07, KGW News (OR)* — **Portland International Airport partially evacuated over bomb scare.** A bomb scare has forced a partial evacuation at Portland International Airport (PDX) after a suspicious bag was found near a lobby area just after noon on Tuesday, March 7. The bag was located in a screening machine in the north ticket lobby, according to Steve Johnson, a spokesperson for PDX. He said as a precaution, airport security closed the north ticket lobby and the north bag claim area below. Everyone was evacuated from those areas as well and ticket counters were closed for United, Delta, Hawaiian, American West, and Continental Airlines. Officials with the Transportation Security Administration called for assistance from a Portland bomb squad, which arrived on the scene with a specialized armored vehicle.
Source: http://www.kgw.com/news-local/stories/kgw_030706_news_airport_evacuation.19442e3.html

[Return to top]

Postal and Shipping Sector

18. *March 07, DMNews* — **UPS boosts delivery speed.** The time it takes for a UPS ground package to reach major cities nationwide just got shorter. UPS has upgraded its U.S. ground package network, accelerating delivery of more than a half-million packages nationwide by one day or more, the Atlanta company officials said on Monday, March 6. The improvements focus on 11 major metropolitan areas such as New York, Chicago, Washington, and the Los Angeles area but affect more than three million ZIP code pairings. The enhancements, made over several months, improve service for 1.2 million customers nationwide without changing pickup and delivery hours.
Source: http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=35974

[Return to top]

Agriculture Sector

19. *March 07, Associated Press* — **New Zealand farms struck by mystery pig disease.** New Zealand farmers on Tuesday, March 7, began testing for known livestock diseases in an effort to identify a mystery illness that is killing piglets on South Island farms, officials said. Pork Industry Board Chief Executive Angus Davidson said the board had sent samples from about six farms with sick pigs in central Canterbury to an independent laboratory for testing. "The symptoms include everything from wasting to death," Davidson said. Industry vets monitoring the farms had been unable to identify the ailment killing young pigs on the farms. The affected pig farms were all in the same area so the disease was spreading via the wind or through bird or pig movement, he said. Ministry of Agriculture and Forestry and other veterinarians had ruled out the worst exotic diseases affecting pigs, Davidson said, adding the board was expecting results from a range of laboratory tests by the end of the week.
Source: http://www.cattlenetwork.com/content.asp?contentid=21353

20. *March 06, Texas A&M AgNews* — **Protecting agriculture requires planning.** Close examination is taking place to determine what is needed to protect the region's approximate $5.7 billion agriculture industry and prepare for a disaster, whether caused by terrorism or from Mother Nature. Private industry, higher education and government agencies are working to build a Panhandle Agro−Security Plan, in conjunction with the state's Foreign and Emerging Animal Disease Response Plan developed by the Texas Animal Health Commission. That the cattle feeding industry in the Texas, Oklahoma and New Mexico region is the largest in the world is no secret, said Bob DeOtte, coordinator of the Panhandle Agro−Security Working Group. Neither is the fact that the dairy industry is growing and an established swine industry also exists here. Less known may be the efforts of a partnership working to establish voluntary plans to protect these vital livestock industries, DeOtte said. The working group consists of officials with West Texas A&M, Texas Agricultural Experiment Station, Texas Cooperative Extension, Texas Veterinary Medical Diagnostic Laboratory, Texas Department of State Homeland Security, agriculture industry, regional law enforcement, emergency management, and county and city governments.
Source: http://agnews.tamu.edu/dailynews/stories/BIOT/Mar0606a.htm

[Return to top]

Food Sector

21. *March 07, U.S. Department of Agriculture* — **Malaysia opens market to U.S. beef products.** Agriculture Secretary Mike Johanns Tuesday, March 7, announced that Malaysia will resume imports of U.S. beef and beef products. Under the agreement, the U.S. will be able to export boneless beef from animals under 30 months of age. U.S. and Malaysian authorities are working to finalize the remaining documentation details so that shipments can begin in the near future. In 2003, the U.S. exported more than $1.9 million worth of beef and beef products to Malaysia. Following the detection of mad cow disease in December 2003, Malaysia imposed a ban on all U.S. beef and beef products.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB/.cmd/ad/.ar/sa.retrievecontent/.c/6_2_1UH/.ce/7_2_5JM/.p/5_2_4TQ/.d/3/_th/J_2_9D/_s.7_0_A/7_0_1OB?PC_7_2_5JM_contentid=2006%2F03%2F0068.xml&PC_7_2_5JM_navtype=RT&PC_7_2_5JM_parentnav=LATEST_RELEASES&PC_7_2_5JM_navid=NEWS_RELEASE#7_2_5JM

22. *March 06, Food Safety and Inspection Service* — **Rule would make retail lists available during recalls.** The Food Safety and Inspection Service (FSIS) Monday, March 6, announced a proposed rule which would make public lists of retail outlets that have received products that have been recalled. When a recall is conducted, FSIS posts a recall press release on its Website. FSIS also distributes the press release to the media in those states where the product has been distributed as well as electronically to mailing lists maintained by FSIS. Federal, state, and local health and agricultural officials are also alerted to the fact that a recall is taking place. The recall release includes the name of the recalling establishment, the reason for the recall, a description of the food being recalled, and any identifying codes, the recall classification. During the recall process, FSIS receives lists of consignees from the recalling firm. FSIS contacts consignees at all levels of distribution. If a product has been distributed to the retail level, under the proposed rule, FSIS will post a complete list of retail outlets on its Website

once that list has been verified for accuracy.
Rule: http://www.fsis.usda.gov/OPPDE/rdad/FSISDirectives/8080.1Rev 4Amend3.pdf
Source: http://www.fsis.usda.gov/News_&_Events/NR_030606_01/index.as p

23. *March 06, U.S. Food and Drug Administration* — **Egg salad sandwiches recalled.** Classic Delight, Inc. of St. Marys, OH, is recalling "Egg Salad on Vienna Bread, Pilot good to go" sandwiches because the product has the potential to be contaminated with Listeria monocytogenes, an organism that can cause serious and sometimes fatal infections in young children, frail or elderly people, and others with weakened immune systems. No illnesses resulting from the consumption of this product have been reported to date. The Egg Salad sandwiches were distributed to Pilot Travel Centers LLC located in the following states: Ohio, Wisconsin, Wyoming, Utah, Nevada, Oregon, Iowa, Montana, Kentucky, Tennessee, North Carolina, Mississippi, Arkansas, West Virginia, New Mexico, Oklahoma, South Dakota, New Jersey, Pennsylvania, Idaho, Florida, Illinois, Colorado, Georgia, New York, Texas, California, Washington, Arizona, and Indiana. The frozen sandwiches are intended to be thawed and sold as a single service item at the Pilot locations.
Source: http://www.fda.gov/oc/po/firmrecalls/classicdelight03_06.htm l

24. *March 06, Reuters* — **Japan says unclear if U.S. beef actions would work.** Japan's vice farm minister said on Monday, March 6, it is unclear if actions proposed by Washington would help prevent shipments of banned U.S. beef to Japan. Japan suspended U.S. beef imports on January 20, just a month after it eased a two−year−old ban on U.S. beef imposed over mad cow disease fears, when Japanese inspectors discovered banned spinal material in a veal shipment from New York. The U.S. Department of Agriculture (USDA) submitted to Japan on February 17 a report that examined how the violation occurred and USDA steps to prevent a repetition. Japan will seek a U.S. explanation about whether USDA properly certifies U.S. meatpacking plants as eligible beef suppliers to Japan, and whether it is properly inspecting such plants. The USDA report said a U.S. firm made an ineligible shipment because the exporter and the USDA inspector were not sufficiently familiar with the requirements of Japan's beef export program. The veal was shipped by Atlantic Veal and Lamb and supplied by Golden Veal, both of which were certified on January 6. USDA personnel confirmed at the time that both understood the requirements of the program.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/03 /06/AR2006030600143.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

25. *March 07, Annals of Internal Medicine* — **Emergence of community−acquired Methicillin−resistant Staphylococcus aureus.** Studies have shown that community−acquired

methicillin−resistant Staphylococcus aureus (CA−MRSA) causes S. aureus skin and soft−tissue infection in selected populations. Researchers sought to determine the proportion of infections caused by CA−MRSA, the clinical characteristics associated with CA−MRSA, and the molecular epidemiology of CA−MRSA among persons with community−onset S. aureus skin and soft−tissue infection. Researchers studied 389 people with microbiologically confirmed community−onset S. aureus skin and soft−tissue infection. Community−onset skin and soft−tissue infection due to S. aureus was identified in 389 episodes, with MRSA accounting for 72 percent. Among all S. aureus isolates, 63 percent were community−acquired MRSA. Among MRSA isolates, 87 percent were CA−MRSA.
CA−MRSA information: http://www.cdc.gov/ncidod/dhqp/ar_mrsa_ca.html
Source: http://www.annals.org/cgi/content/abstract/144/5/309

26. *March 07, Agence France−Presse* — **Malaysia fights to contain hand, foot and mouth disease.** Malaysian health officials said they would shut more kindergartens if necessary to prevent an outbreak of hand, foot and mouth disease in eastern Sarawak state from spreading nationwide. Four children have died and thousands of others have received medical attention so far this year because of the virus. Malaysia's Health Minister Chua Soi Lek said the government was on alert for the spread of the disease from Sarawak, located on Borneo Island, into peninsular Malaysia, where most of the country's population live. "If more than two children in a kindergarten are infected, it will be shut down automatically to break the chain of transmission," Chua said. The health ministry on Friday, March 3, ordered the immediate closure of 488 Sarawak kindergartens for two weeks to curb the spread of the disease. Sarawak health director Yao Sik King said as many as 200 new cases were being reported daily. Yao said that a total of 3,087 cases had been recorded since January 1. Some 80 percent of the patients were children aged below six years, he added. The disease mostly affects infants and young children. Symptoms include fever, mouth ulcers and rashes.
Source: http://www.todayonline.com/articles/105130.asp

27. *March 07, CNN* — **U.S. developing new bird flu vaccine.** A second vaccine against the H5N1 bird flu virus is under development, Health and Human Services Secretary Michael Leavitt said Monday, March 6. The National Institutes of Health (NIH) has already developed and tested one vaccine against H5N1 based on the virus found in Vietnam. So far, eight million doses of this vaccine have been produced. The new vaccine would use a strain of the H5N1 virus found in Indonesia. Scientists at the Centers for Disease Control and Prevention (CDC), with researchers in Hong Kong, have determined that the first NIH−developed vaccine is not effective against the strain circulating in Indonesia. The virus continues to change and that the CDC has found a "seed" virus of the new form of H5N1, and it will be used for the next vaccine. One of the researchers who isolated the new strain of H5N1, Reuben Donis, said the discovery of a new strain does not render the first eight million doses useless. He explained that there are at least two groups of the H5N1 virus. One comes from Vietnam and the second comes from Indonesia, while there also may be a couple of other groups.
Source: http://edition.cnn.com/2006/HEALTH/03/06/birdflu.vaccine/

28. *March 07, Reuters* — **World Health Organization urges more studies on bird flu infections in cats.** Reports that a cat contracted bird flu and has not fallen ill could mean the virus is adapting to mammals and poses a potentially higher risk to humans, a World Health Organization (WHO) official said on Tuesday, March 7. Michael Perdue, a scientist with the

WHO's global influenza program, said more studies were needed on infections in cats, including how they shed the virus. But Perdue said there was no current evidence that cats were hidden carriers of a virus. Austria said on Monday, March 6, that a cat in an animal sanctuary in the southern city of Graz had tested positive for the H5N1 bird flu virus but had yet to show any symptoms of the disease. However, the virus can take up to a week to strike and perhaps the cat in Austria could still develop clinical signs, according to Perdue. "We have to follow−up with laboratory studies to see if it (the virus) changed genetically and is not causing clinical signs," Perdue told Reuters. "If it is true, it would imply the virus has changed significantly," he said.
Source: http://www.alertnet.org/thenews/newsdesk/L07562908.htm

29. *March 07, Reuters* — **Food and Agriculture Organization to boost bird flu role.** The United Nations' Food and Agriculture Organization (FAO) is to play a greater role in fighting bird flu, becoming a "global clearing house" for efforts to stem the spread of the virus, it said on Tuesday, March 7. The U.S. and the European Union (EU) have backed the formation of a what a senior U.S. official called an "emergency operations center" at the FAO's Rome, Italy, headquarters. The initiative was agreed at a meeting at the FAO requested by the U.S. and EU. Funding for the center will come from a pot of almost two billion dollars pledged by wealthy nations at an international conference in China in January. The U.S. would provide experts to help run the center and expects other nations to follow suit. The move follows the spread of H5N1 avian flu into at least 15 new nations over the past month, with cases detected in birds in several countries across Europe and also in flocks in Egypt and West Africa. The virus, which re−emerged in Asia in late 2003, can wipe out poultry flocks in the space of 48 hours. It can also infect people who come into close contact with sick poultry and has claimed 95 human lives.
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=healthNews&storyID=2006−03−07T182320Z_01_L05348852_RTRIDST_0_HEALTH−BIRDFLU−DC.XML&archived=False

30. *March 06, Agence France−Presse* — **Serbia confirms first case of H5N1 bird flu.** Serbia's health authorities confirmed its first cases of the H5N1 virus in at least two swans found dead in northern and western parts of the country. "Based on results from tests we have carried out, it is H5N1," the director of the Veterinary Institute of Serbia, Dejan Krnjaic, said, adding that samples were sent to a laboratory in Britain for full confirmation. "Both tested swans from the northern locality of Backi Monostor and from the western village of Bacevci were positive for H5N1," Krnjaic added. One of the swans was found at Backi Monostor on Thursday, March 2, less than six miles from the Serbian border with Croatia and Hungary. Another was discovered at the weekend near Bacevci village on the River Drina, which is the natural border between Serbia and Bosnia. The H5N1 virus has been detected in a number of countries neighboring Serbia, including Bosnia, Croatia, and Hungary.
Source: http://news.yahoo.com/s/afp/20060306/hl_afp/healthfluserbia_060306163006;_ylt=AuKDMbGnd9A1DnJ.2_khs_aJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

31. *March 06, RIA Novosti (Russia)* — **Bird flu registered in eight Russian regions.** The Russian Agriculture Ministry said Monday, March 6, that bird flu has now been registered in eight Russian regions, all in the southern part of the country, a major stopover area for migrating birds. The ministry said that, according to data gathered by its agriculture watchdog, cases of

bird flu had been registered in the republics of Kabardino−Balkaria, Dagestan, Chechnya, Kalmykia, Adygea, North Ossetia−Alania, and in the Krasnodarsk and Stavropol Territories. Outbreaks among domestic birds have occurred in five areas: the Krasnodarsk and Stavropol Territories, Dagestan, Adygea, and Kalmikia. The Emergency Situations Ministry also announced a suspected outbreak of bird flu in the Astrakhan Region, also in southern Russia. Over 1.3 million birds have died or been slaughtered in three outbreaks of bird flu since July 2005, or over 44,000 every day, the ministry said. This includes more than 416,000 birds, or about 17,500 every day, that died from the virus.
Source: http://en.rian.ru/russia/20060306/43966945.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

32. *March 06, Daily Breeze (CA)* — **Computer program in the works for first responder training.** Milind Tambe, an associate professor in the University of Southern California (USC) Department of Computer Science, is leading a computer−modeling effort to create a program that simulates macro−disasters on a citywide scale in conjunction with the Los Angeles Fire Department. Funding comes from USC−based CREATE −− the Center for Risk and Economic Analysis of Terrorism Events −− the first university center in the nation backed by money from the Department of Homeland Security. The idea behind CREATE is to develop tools emergency responders can use to protect lives and property in the aftermath of a disaster such as a major terrorist strike. "What we're focusing on is the resource allocation problem: What personnel should be assigned to what kind of task?" said doctoral student Nathan Schurr, who is co−developing this project. Tambe and Schurr's program, based upon the city of Kobe, Japan, which was devastated by a magnitude 7.2 earthquake in 1995, has 400 buildings and as many as 20 fire engines, each a different software agent. By summer, Tambe hopes to replace the simulated city of Kobe with Los Angeles, using geographic information systems data provided by city officials.
Source: http://www.dailybreeze.com/news/articles/2411511.html?showAl l=y&c=y

33. *March 06, Texas Engineering Extension Service* — **Leading incident management training center in Texas doubles size.** The Texas Engineering Extension Service's National Emergency Response and Rescue Training Center is doubling the size of its Emergency Operations Training Center (EOTC), which serves as the home of one of the nation's top courses for computer−simulated incident management training. The 17,000−square−foot EOTC expansion, which should be completed in early 2008, includes the construction of a fully functioning Emergency Operations Center, observation decks for exercise controllers, and two parking pads for mobile incident command units. The expansion will allow for a simulation exercise to be conducted with the command post and operations center at the same time.
Source: http://www.teex.com/teex.cfm?pageid=media&area=teex&template

id=23&storyid=540

34. *March 06, Corpus Christi Caller−Times (TX)* — **Texas officials begin review of hurricane escape plans.** Coastal Bend, TX, officials have banded together to review and revise plans that would help residents leave quickly should a storm threaten the area. Coastal Bend is a region of Texas that includes the following communities: Alice, Aransas Pass, Beeville, Bishop, Corpus Christi, Cuero, George West, Goliad, Ingleside, Jackson County, Kenedy, Kingsville, Padre Island, Palacios, Port Aransas, Port Lavaca, Portland, Refugio, Robstown, Rockport−Fulton, Sinton, Three Rivers, Victoria, and Yorktown. With the havoc wreaked by Hurricanes Katrina and Rita, there's an added pressure to make things better, according to John Murray, the Emergency Management Services director with the city of Corpus Christi. Gov. Rick Perry has said he plans to ask the Legislature to give him the power to call for mandatory evacuations rather than wait for county judges, where the power currently rests. William Zagorski, who coordinates emergency management for San Patricio County, said he and his counterparts in the region are working to shift to a phased evacuation in which stores stay open longer and transient people leave first. In addition, groups are being assembled to handle everything from debris management to food, water and ice distribution to volunteer coordination and donation management.
Source: http://www.caller.com/ccct/local_news/article/0,1641,CCCT_81 1_4518363,00.html

35. *March 06, Associated Press* — **FCC chief, others focus on hurricane communication problems.** A lack of reliable communications during and after Hurricane Katrina left emergency responders confused and isolated, experts told federal regulators on Monday, March 6. Federal Communications Commission (FCC) Chairman Kevin Martin said three million telephone lines were knocked out by the violent storm that rolled ashore August 29. In states hit by Katrina, he said at least 38 911 call centers went down and more than 1,000 cellular towers were out of service. He said as many as 20,000 calls failed to go through the day after the storm, and about 100 TV and radio stations were knocked off the air. Martin was in Jackson, MS, with an independent panel to gather information that will be presented to the FCC in June. The FCC chairman hopes the panel can gather information to be used to strengthen communications throughout the nation and especially in areas vulnerable to natural disasters.
Source: http://www.sunherald.com/mld/sunherald/news/state/14031984.h tm

[Return to top]

Information Technology and Telecommunications Sector

36. *March 07, IDG News Service* — **Cisco acquires surveillance company.** Cisco Systems on Tuesday, March 7, announced it will acquire SyPixx Networks for $51 million in cash and options. The acquisition will allow Cisco customers to integrate their existing video surveillance systems into an overall physical security program, Cisco said.
Source: http://www.infoworld.com/article/06/03/07/76168_HNciscobuyss urveillance_1.html

37. *March 07, IDG News Service* — **China malware increasing, Symantec says.** The amount of malware coming from China rose 153 percent in the last six months of 2005, Symantec reported Tuesday, March 7. The increase came in remote−controlled "bot" attacks emanating

from China during the period, said Dave Cole, a director with Symantec Security Response. Rising Internet use in China, and a lack of precautions taken by new users, may be contributing to the malware jump.
Source: http://www.infoworld.com/article/06/03/07/76162_HNchinamalwa re_1.html

38. *March 07, Reuters* — **Report: Cyber criminals stepping up targeted attacks.** Cyber criminals are stepping up smaller, more targeted attacks as they seek to avoid detection and reap bigger profits by stealing personal and financial information, according to a report issued on Monday, March 6. Symantec Corp.'s Internet Security Threat report said during the second half of 2005, attackers continued to move away from broad attacks seeking to breach firewalls and routers and are now taking aim at the desktop and Web applications. The latest report said threats such as viruses, worms and Trojans that can unearth confidential information from a user's computer rose to 80 percent of the top 50 malicious software code threats from 74 percent in the previous six months.
Source: http://today.reuters.com/news/articlenews.aspx?type=technolo gyNews&storyid=2006−03−07T061445Z_01_N06313562_RTRUKOC_0_US− SYMANTEC−SECURITY.xml

39. *March 07, CNET News* — **Mac OS X patch faces scrutiny.** An Apple Computer patch released last Wednesday, March 1, that doesn't completely fix a high−profile Mac OS X flaw, leaving a toehold for cyber attacks, experts said. The update added a function called "download validation" to the Safari Web browser, Apple Mail client, and iChat instant messaging tool. The function warns people that a download could be malicious when they click on the link. Before that change, clicking on a link could have resulted in the automatic execution of code on a Mac. But Apple failed to address a key part of the problem; the fix should be at a lower, operating system level, experts said. It is now still possible for hackers to construct a file that appears to be a safe file type, such as an image or movie, but is actually an application, they said.
Source: http://news.com.com/Mac+OS+X+patch+faces+scrutiny/2100−1002_ 3−6046588.html?tag=cd.top

40. *March 06, IDG News Service* — **Researcher hacks Microsoft Fingerprint Reader.** A security researcher with the Finnish military has shown how they could steal your fingerprint, by taking advantage of an omission in Microsoft Corp.'s Fingerprint Reader, a PC authentication device that Microsoft has been shipping since September 2004. Although the Fingerprint Reader can prevent unauthorized people from logging on to your PC, Microsoft has not promoted it as a security device. Hoping to understand why Microsoft had included the caveat about sensitive data, a researcher with the Finnish military, Mikko Kiviharju, took a close look at the product. In a paper presented at the Black Hat Europe conference last week, he reported that because the fingerprint image taken by the scanner is not encrypted, it could be stolen by hackers and used to inappropriately log in to a computer. Because the fingerprint image is transferred unencrypted from the Fingerprint Reader to the PC, it could be stolen using a variety of hardware and software technologies, called "sniffers," that monitor such traffic, said Kiviharju.
Kiviharju's report: http://www.blackhat.com/presentations/bh−europe−06/bh−eu−06− Kiviharju/bh−eu−06−kiviarju.pdf.
Source: http://www.computerworld.com/securitytopics/security/holes/s tory/0,10801,109276,00.html

41. *March 06, Government Computer News* — **Open−source bug hunt results posted.** Coverity Inc. of San Francisco, CA, has released the results of a Department of Homeland Security (DHS)−funded bug hunt that ranged across 40 popular open−source programs. The company found less than one−half of one bug per thousand lines of code on average, and found even fewer defects in the most widely used code, such as the Linux kernel and the Apache Web server. To test the programs, Coverity deployed analysis software first developed by Stanford's computer science department. Ben Chelf, chief technology officer of Coverity, warned that this automated bug scan is not definitive, but it can point to bugs traditional in−house code review techniques can miss. The results are the first deliverable of a $1.2 million, three−year grant DHS awarded to a team consisting of Coverity, Stanford University and Symantec Corp. of Cupertino, CA. DHS wants to reinforce the quality of open−source programs supporting the U.S. infrastructure.
Source: http://www.gcn.com/online/vol1_no1/40053−1.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of publicly available exploit code for a vulnerability in Apple Safari Browser. The Apple Safari browser will automatically open "safe" file types, such as pictures, movies, and archive files. A system may be compromised if a user accesses an HTML document that references a specially crafted archive file. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary commands with the privileges of the user.

More information can be found in the following US−CERT Vulnerability Note:

VU#999708 − Apple Safari may automatically execute arbitrary shell commands
http://www.kb.cert.org/vuls/id/999708

Although there is limited information on how to fully defend against this exploit, US−CERT recommends the following mitigation:

Disable the option "Open 'safe' files after downloading," as specified in the Securing Your Web Browser document.
http://www.us−cert.gov/reading_room/securing_browser/#sgener al

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 8227 (−−−), 6881 (bittorrent), 445 (microsoft−ds), 25 (smtp), 5817 (−−−), 139 (netbios−ssn), 3857 (−−−), 41170 (−−−), 80 (www)

	Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.

[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer